

PATENT ABSTRACTS OF JAPAN

(11) Publication number :

2001-051903

(43) Date of publication of application : **23.02.2001**

(51) Int. Cl.

G06F 12/14

G06F 12/00

G06K 17/00

G06K 19/073

(21)Application number : 11-222351

(71)Applicant : **SONY CORP**

(22) Date of filing : 05.08.1999

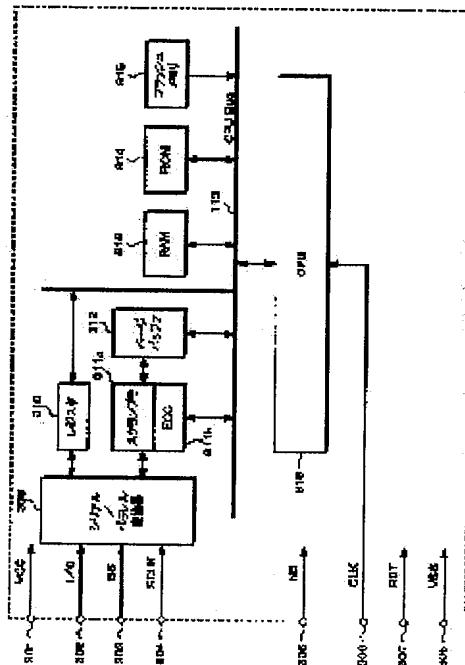
(72)Inventor : IMURA SHIGERU

(54) SEMICONDUCTOR STORAGE DEVICE AND OPERATION SETTING METHOD FOR SEMICONDUCTOR STORAGE DEVICE

(57) Abstract:

PROBLEM TO BE SOLVED: To increase security and to obtain compatibility with memory cards now in use by providing a ciphering means which ciphers data stored in a nonvolatile semiconductor memory and a control means which controls the ciphering.

SOLUTION: Serial data are converted into parallel data in a serial/parallel converter 309 through a bidirectional data communication line I/O between a memory stick which is made intelligent and an external device. To cipher and store the data, a scrambler 311a is supplied with plaintext data and a cipher key and generates ciphered data through specific ciphering algorithm and finally stores them in a flash memory 315. The data are possibly not ciphered and stored in the flash memory 315 in the form of the plaintext data when necessary. Thus, the data are ciphered and stored in the flash memory 315, so the security of the stored data is enhanced.



(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2001-51903

(P2001-51903A)

(43)公開日 平成13年2月23日 (2001.2.23)

(51)Int.Cl.⁷
G 0 6 F 12/14識別記号
3 2 0F I
G 0 6 F 12/14テ-マコ-ト(参考)
3 2 0 B 5 B 0 1 7
3 2 0 C 5 B 0 3 5

3 1 0

3 1 0 E 5 B 0 5 8
3 1 0 K 5 B 0 8 2

12/00

5 3 7

12/00

5 3 7 H

審査請求 未請求 請求項の数38 OL (全 21 頁) 最終頁に統く

(21)出願番号 特願平11-222351

(71)出願人 000002185

ソニー株式会社

(22)出願日 平成11年8月5日 (1999.8.5)

東京都品川区北品川6丁目7番35号

(72)発明者 井村 滉

東京都品川区北品川6丁目7番35号 ソニー
株式会社内

(74)代理人 100082762

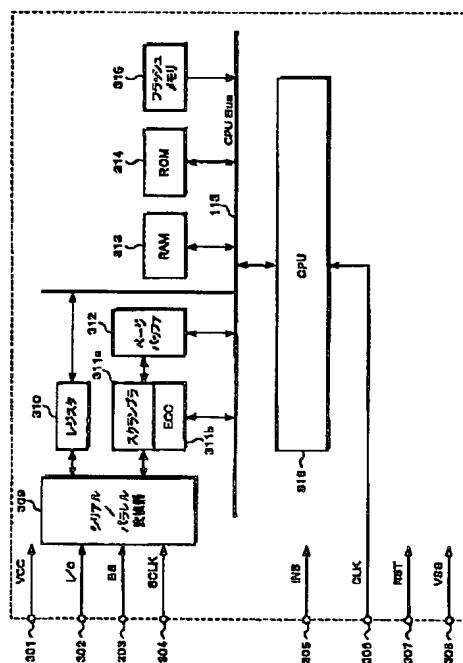
弁理士 杉浦 正知

(54)【発明の名称】 半導体記憶装置及び半導体記憶装置の動作設定方法

(57)【要約】

【課題】 セキュリティを高めることができると共に、現行のメモリカードとの互換性を図れるようにした半導体記憶装置及び半導体記憶装置の動作設定方法を提供する。

【解決手段】 メモリスティックの構成のメモリカードに、CPUと、暗号化回路が設けられる。入出力されるデータは、暗号化されて、フラッシュメモリに記憶される。メモリスティックをアクセスするための命令体系には、公開された命令体系と非公開の命令体系とを有している。フラッシュメモリに記憶されるファイルデータは、各ファイルデータ毎に、アクセス制限、コピーガード情報、及びアクセス時の暗号化、暗証番号を選択的に設定できる。これらのファイルデータは、隠されたデータファイルを含むデータファイルが処理を管理している。また、ファイルデータにはアクセス権が設定され、アクセス権に従って、ファイルデータの読み出し及び書き込みのアクセスが制限される。このように、データが暗号化されてフラッシュメモリに記憶されるため、記憶されるデータのセキュリティが強化される。



(2)

特開2001-51903

【特許請求の範囲】

【請求項1】 不揮発性半導体メモリと、上記不揮発性半導体メモリに対するデータの入出力の制御を行なうデータ入出力制御手段と、外部機器とのインターフェース手段とからなるメモリカードの構成の半導体記憶装置に対して、上記不揮発性半導体メモリに記憶するデータを暗号化する暗号化手段と、上記暗号化を制御する制御手段とを設けるようにした半導体記憶装置。

【請求項2】 上記不揮発性メモリをアクセスするための命令体系には、公開された命令体系と非公開の命令体系とを有するようにした請求項1に記載の半導体記憶装置。

【請求項3】 上記不揮発性半導体メモリに記憶されるファイルデータは、隠されているファイルデータを含む請求項1に記載の半導体記憶装置。

【請求項4】 上記不揮発性半導体メモリに記憶されるファイルデータは、各ファイルデータ毎に、アクセス制限、コピーガード情報、及びアクセス時の暗号化、暗証番号を選択的に設定できるようにした請求項1に記載の半導体記憶装置。

【請求項5】 上記不揮発性半導体メモリに記憶されるファイルデータは、隠されたデータファイルを含むデータファイルが処理を管理するようにした請求項4に記載の半導体記憶装置。

【請求項6】 上記不揮発性半導体メモリに記憶されるファイルデータにはアクセス権が設定され、上記アクセス権に従って、上記ファイルデータの読み出し及び書き込みのアクセスが制限される請求項1に記載の半導体記憶装置。

【請求項7】 上記アクセス権の制限は、ユーザの暗証番号により設定できる請求項1に記載の半導体記憶装置。

【請求項8】 上記制御手段の作動クロックと、データ入出力に使用される転送クロックが独立して変更可能とされた請求項1に記載の半導体記憶装置。

【請求項9】 上記制御手段の作動クロックを分周して、データ入出力の転送クロックとして使用するようにした請求項1に記載の半導体記憶装置。

【請求項10】 上記暗号化手段は、個人情報のパラメータに基づいて暗号化キーを発生するようにした請求項1に記載の半導体記憶装置。

【請求項11】 上記暗号化手段は、ユーザの暗証番号に基づいて暗号化キーを発生するようにした請求項1に記載の半導体記憶装置。

【請求項12】 上記暗号化手段は、加入者番号に基づいて暗号化キーを発生するようにした請求項1に記載の半導体記憶装置。

【請求項13】 上記暗号化手段は、上記個人情報のパラメータと、上記非公開の管理用の命令体系でアクセスされるパラメータに基づいて暗号化キーを発生するよう

にした請求項1に記載の半導体記憶装置。

【請求項14】 上記暗号化手段は、暗号化アルゴリズムにより生成された暗号化キーと変化する値とを複合した値を暗号化キーとするようにした請求項1に記載の半導体記憶装置。

【請求項15】 上記変化する値は、ページモードをアクセスする際のページ番号である請求項14に記載の半導体記憶装置。

【請求項16】 上記不揮発性半導体メモリに入力データを暗号化して記憶すると共に上記不揮発性半導体メモリから読み出されたデータを解読して出力するようにした請求項1に記載の半導体記憶装置。

【請求項17】 上記不揮発性半導体メモリに入力データを暗号化して記憶すると共に上記不揮発性半導体メモリから読み出されたデータを解読して出力するモードと、上記不揮発性半導体メモリに入力データをそのまま記憶すると共に上記不揮発性半導体メモリから読み出されたデータをそのまま出力するモードとが設定可能とされた請求項1に記載の半導体記憶装置。

【請求項18】 上記不揮発性半導体メモリに入力データを暗号化して記憶すると共に上記不揮発性半導体メモリから読み出されたデータを解読して出力するモードと、上記不揮発性半導体メモリに入力データを暗号化して記憶すると共に上記不揮発性半導体メモリから読み出された暗号化されたデータを出力するモードを備えるようにした請求項1に記載の半導体記憶装置。

【請求項19】 上記不揮発性半導体メモリに入力データを暗号化して記憶すると共に上記不揮発性半導体メモリから読み出されたデータを解読して出力するモードと、上記不揮発性半導体メモリに入力データをそのまま記憶すると共に上記不揮発性半導体メモリから読み出されたデータをそのまま出力するモードと、上記不揮発性半導体メモリに入力データを暗号化して記憶すると共に上記不揮発性半導体メモリから読み出された暗号化されたデータを出力するモードを備えるようにした請求項1に記載の半導体記憶装置。

【請求項20】 不揮発性半導体メモリと、上記不揮発性半導体メモリに対するデータの入出力の制御を行なうデータ入出力制御手段と、外部機器とのインターフェース手段とからなるメモリカードの構成の半導体記憶装置に対して、データを暗号化し、上記暗号化されたデータを上記不揮発性半導体メモリに記憶するようにした半導体記憶装置の動作設定方法。

【請求項21】 上記不揮発性メモリをアクセスするための命令体系には、公開された命令体系と非公開の命令体系とを有するようにした請求項20に記載の半導体記憶装置の動作設定方法。

【請求項22】 上記不揮発性半導体メモリに記憶されるファイルデータは、隠されているファイルデータを含む請求項20に記載の半導体記憶装置の動作設定方法。

(3)

特開2001-51903

【請求項23】 上記不揮発性半導体メモリに記憶されるファイルデータは、各ファイルデータ毎に、アクセス制限、コピーガード情報、及びアクセス時の暗号化、暗証番号を選択的に設定できるようにした請求項20に記載の半導体記憶装置の動作設定方法。

【請求項24】 上記不揮発性半導体メモリに記憶されるファイルデータは、隠されたデータファイルを含むデータファイルが処理を管理するようにした請求項23に記載の半導体記憶装置の動作設定方法。

【請求項25】 上記不揮発性半導体メモリに記憶されるファイルデータにはアクセス権が設定され、上記アクセス権に従って、上記ファイルデータの読み出し及び書き込みのアクセスが制限される請求項20に記載の半導体記憶装置の動作設定方法。

【請求項26】 上記アクセス権の制限は、ユーザの暗証番号により設定できる請求項20に記載の半導体記憶装置の動作設定方法。

【請求項27】 上記制御手段の作動クロックと、データ入出力に使用される転送クロックが独立して変更可能とされた請求項20に記載の半導体記憶装置の動作設定方法。

【請求項28】 上記制御手段の作動クロックを分周して、データ入出力の転送クロックとして使用するようにした請求項20に記載の半導体記憶装置の動作設定方法。

【請求項29】 上記暗号化手段は、個人情報のパラメータに基づいて暗号化キーを発生するようにした請求項20に記載の半導体記憶装置の動作設定方法。

【請求項30】 上記暗号化手段は、ユーザの暗証番号に基づいて暗号化キーを発生するようにした請求項20に記載の半導体記憶装置の動作設定方法。

【請求項31】 上記暗号化手段は、加入者番号に基づいて暗号化キーを発生するようにした請求項20に記載の半導体記憶装置の動作設定方法。

【請求項32】 上記暗号化手段は、上記個人情報のパラメータと、上記非公開の管理用の命令体系でアクセスされるパラメータに基づいて暗号化キーを発生するようにした請求項20に記載の半導体記憶装置の動作設定方法。

【請求項33】 上記暗号化手段は、暗号化アルゴリズムにより生成された暗号化キーと変化する値とを複合した値を暗号化キーとするようにした請求項20に記載の半導体記憶装置の動作設定方法。

【請求項34】 上記変化する値は、ページモードをアクセスする際のページ番号である請求項33に記載の半導体記憶装置の動作設定方法。

【請求項35】 上記不揮発性半導体メモリに入力データを暗号化して記憶すると共に上記不揮発性半導体メモリから読み出されたデータを解読して出力するようにした請求項20に記載の半導体記憶装置の動作設定方法。

【請求項36】 上記不揮発性半導体メモリに入力データを暗号化して記憶すると共に上記不揮発性半導体メモリから読み出されたデータを解読して出力するモードと、上記不揮発性半導体メモリに入力データをそのまま記憶すると共に上記不揮発性半導体メモリから読み出されたデータをそのまま出力するモードとが設定可能とされた請求項20に記載の半導体記憶装置の動作設定方法。

【請求項37】 上記不揮発性半導体メモリに入力データを暗号化して記憶すると共に上記不揮発性半導体メモリから読み出されたデータを解読して出力するモードと、上記不揮発性半導体メモリに入力データを暗号化して記憶すると共に上記不揮発性半導体メモリから読み出された暗号化されたデータを出力するモードを備えるようにした請求項20に記載の半導体記憶装置の動作設定方法。

【請求項38】 上記不揮発性半導体メモリに入力データを暗号化して記憶すると共に上記不揮発性半導体メモリから読み出されたデータを解読して出力するモードと、上記不揮発性半導体メモリに入力データをそのまま記憶すると共に上記不揮発性半導体メモリから読み出されたデータをそのまま出力するモードと、上記不揮発性半導体メモリに入力データを暗号化して記憶すると共に上記不揮発性半導体メモリから読み出された暗号化されたデータを出力するモードを備えるようにした請求項20に記載の半導体記憶装置の動作設定方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 この発明は、特に、ネットワークを介して配信されてくるコンテンツのデータを保存するのに用いて好適な半導体記憶装置及び半導体記憶装置の動作設定方法に関する。

【0002】

【従来の技術】 インターネットを使って、音楽データを配信するようなサービスが開始されている。このようなサービスでは、インターネット上に、音楽データを配信するようなサイトが設けられる。ユーザはこのサイトをアクセスして、所望の楽曲を選択すると、選択された音楽データがインターネットを介して送られ、記録媒体にダウンロードされる。

【0003】 また、デジタル衛星放送を使って音楽配信を行なうようなサービスが提案されている。このようなサービスでは、音楽チャンネルで、その番組を提供する映像データや音声データと共に、付加データとして、ダウンロード用の音楽データと、ダウンロード用の画面を形成するためのMHEG (Multimedia and Hypermedia Information Coding Experts Group) やXML (eXtensible Markup Language) 等のスクリプト言語のデータが送られてくる。このスクリプト言語のデータにより、ダウンロード用の画面が形成され、この画面上から指示

(4)

特開2001-51903

を与えると、ダウンロード用として送られてきた音楽データが記録媒体にダウンロードされる。

【0004】更に、携帯電話を使って音楽配信を行うようにしたサービスが提案されている。このようなサービスでは、携帯電話に音楽配信サービスを提供するダイアルが設けられる。携帯電話で所定のダイアル番号に接続すると、音楽データの配信サービスを受けることができる。携帯電話を操作すると、所望の音楽データが携帯電話の回線網を介して送られ、この音楽データが携帯電話に装着された記録媒体にダウンロードされる。

【0005】

【発明が解決しようとする課題】このように、インターネットやデジタル衛星放送、携帯電話回線等、種々の伝送媒体を使って、音楽データ、出版物、ゲームのソフトウェア等のコンテンツを提供するサービスが考えられている。そして、このようなサービスでは、送られてきたデータが記録媒体にダウンロードされる。

【0006】このように、コンテンツのデータをダウンロードするための記録媒体としては、フロッピディスクやハードディスク等の磁気ディスク、或いは、CD-R (CD-Recordable) やMO (Magneto-Optical) のような光ディスク又は光磁気ディスクを用いることが考えられる。ところが、このようなディスク状の記録媒体は、機構部を含むため、耐震性に問題があり、また、大型化し、外部に携帯したり、手軽に使用するのは困難である。

【0007】そこで、このようなコンテンツのデータをダウンロードするための記録媒体として、メモリスティックと称されるメモリカードを用いることが提案されている。

【0008】メモリスティックは、NAND型のフラッシュメモリを用いたカード型の不揮発性半導体メモリである。このメモリスティックは、従来から広く使われているPCMCIA (Personal Computer Memory Card International Association) インターフェースを利用したパラレルインターフェースではなく、シリアルの半二重同期データ転送方式を利用して20MB/s程度のアクセス速度を有しており、高速アクセスが可能で、メモリ容量もおよそ64MB程度まで計画されている。この64MBというメモリスティックの容量は、既存のフロッピディスクの記憶容量(1.4MB)よりも大きく、コンテンツのデータを記録するのには十分な容量であると考えられる。また、この容量は、MD (Mini Disc) やCD-Rの記憶容量(128MBから640MB)より小容量ではあるが、MDやCD-Rは機構部を含み大型化し、手軽に扱えないのに対して、メモリスティックは、小型で扱いが容易であり、耐震性に優れている。

【0009】例えば、音楽データをダウンロードするような場合には、ユーザは、このダウンロードした音楽データを携帯型のヘッドホンステレオで再生したり、カ

オーディオで再生することが考えられる。このような使用方法では、小型で、耐震性が優れたメモリスティックは、非常に有用な記録媒体であると考えられる。

【0010】ところが、メモリスティックは、現状では、CPUは内蔵されておらず、セキュリティ機能が万全であるとは言えない。音楽データをダウンロードするような場合には、著作権を保護する上から、セキュリティを高める必要がある。特に、ネットワークを利用してこれらのコンテンツのデータを取得する際に、電子マネーを使って、課金を行なうことが考えられている。メモリスティックでは、CPUが内蔵されていないため、このような課金処理が困難である。

【0011】また、CPUが内蔵されたカードとしては、ICカードが知られている。例えば、ヨーロッパのGSM (Group Special Mobile) 方式の携帯電話では、ISO7816に準拠したSIMと呼ばれるICカードが用いられている。このICカードは、GSM方式の携帯電話で、認証、契約内容、暗号アルゴリズム、短縮ダイアル等を記憶するのに使われている。また、ペイテレピジョンや、モンデックスシステムのような電子マネーで、CPU内蔵のICカードが使われている。このようなICカードは、メモリカードに比較して、複製、偽造に対して高い守秘性がある。

【0012】しかしながら、これらのICカードは、メモリ容量が小さく、アクセス速度も遅いため、ダウンロードしたコンテンツを保存しておくような用途に使用することは困難である。

【0013】したがって、この発明の目的は、セキュリティを高めることができると共に、現行のメモリカードとの互換性を図れるようにした半導体記憶装置及び半導体記憶装置の動作設定方法を提供することにある。

【0014】

【課題を解決するための手段】この発明は、不揮発性半導体メモリと、不揮発性半導体メモリに対するデータの入出力の制御を行なうデータ入出力制御手段と、外部機器とのインターフェース手段とからなるメモリカードの構成の半導体記憶装置に対して、不揮発性半導体メモリに記憶するデータを暗号化する暗号化手段と、暗号化を制御する制御手段とを設けるようにした半導体記憶装置である。

【0015】この発明は、不揮発性半導体メモリと、不揮発性半導体メモリに対するデータの入出力の制御を行なうデータ入出力制御手段と、外部機器とのインターフェース手段とからなるメモリカードの構成の半導体記憶装置に対して、データを暗号化し、暗号化されたデータを不揮発性半導体メモリに記憶するようにした半導体記憶装置の動作設定方法である。

【0016】メモリスティックの構成のメモリカードに、CPUと、暗号化回路が設けられる。そして、入出力されるデータは、暗号化されて、フラッシュメモリに

(5)

特開2001-51903

記憶される。また、メモリスティックをアクセスするための命令体系には、公開された命令体系と非公開の命令体系とを有している。フラッシュメモリに記憶されるファイルデータは、各ファイルデータ毎に、アクセス制限、コピーガード情報、及びアクセス時の暗号化、暗証番号を選択的に設定できる。これらのファイルデータは、隠されたデータファイルを含むデータファイルが処理を管理している。また、ファイルデータにはアクセス権が設定され、アクセス権に従って、ファイルデータの読み出し及び書き込みのアクセスが制限される。このように、データが暗号化されてフラッシュメモリに記憶されるため、記憶されるデータのセキュリティが強化される。

【0017】

【発明の実施の形態】この発明の実施の形態について以下の順序で説明する。

【0018】1. SIMの内部構成

2. メモリスティックの内部構成

3. スマートスティックの一例

3-1. スマートスティックの一例の構成

3-2. 外部装置とスマートスティックとのセッション

3-3. 暗号化について

3-4. ファイル構成について

3-5. アクセス処理について

4. インテリジェント化されたメモリスティックの他の例。

【0019】1. SIMの内部構成

この発明は、SIMと呼ばれるICカードの機能をメモリスティックと呼ばれるメモリカードに付加することで、セキュリティを高めることができると共に、現行のメモリスティックとの互換性を図るためにしたものである。本願の説明に先立ち、SIMと呼ばれるICカードと、メモリスティックと呼ばれるメモリカードについて説明する。

【0020】SIMと呼ばれるICカードは、ISO (International Organization for Standardization) 7.8.1.6に準拠したCPU内蔵のICカードであり、GSM (Group Special Mobile) 方式の携帯電話で、加入者の暗号番号により認証、契約内容暗号アルゴリズム、短縮ダイアル番号等を記憶するのに用いられている。

【0021】図1はSIMと呼ばれるICカードの内部構成を示すブロック図である。このICカードには、外部機器との接続端子として、電源端子101と、プログラム用電源端子102と、双方向データの入出力端子103と、クロック入力端子104と、リセット入力端子105と、接地端子106とが設けられる。

【0022】電源端子101は、作動電源Vccを外部から供給するためのものである。作動電源Vccの電圧は5V或いは3Vである。

【0023】プログラム電源端子102は、内蔵されて

いるEEPROM (Electrically Erasable and Programmable ROM) 110に、プログラム用電源Vppを供給するためのものである。EEPROM 110は、電子的消去可能な不揮発性メモリである。このEEPROM 110に与えられるプログラム用電源Vppの電圧は、一般的に、電源電圧Vccと同様とされている。また、SIMの内部でプログラム用電源Vppが発生されているものもある。ここでは、外部から供給する構造を示しているが、これは重要ではない。

【0024】双方向データの入出力端子103は、双方向データ信号線I/Oにより実際にデータの入出力を行なうためのデータ入/出力端子である。双方向データ信号線I/Oには、シリアル/パラレル変換器107を介して、データが入/出力される。このデータ信号線I/Oは、入力或いは出力されていないときには、作動電源の電圧Vccと略同じ電圧に維持されており、外部の制御機器及びSIMは、互いにデータ受信状態となってい

る。

【0025】クロック入力端子104には、クロックCLKが供給される。このクロックCLKは、SIMに内蔵されているCPU (Central Processing Unit) 112の作動用クロックである。また、このクロックCLKは、分周器108で適当に分周されて、シリアル/パラレル変換器107に供給される。この分周器108で分周されたクロックCLKは、双方向データ信号線I/Oで交換されるデータの転送速度を決める転送クロックとなる。

【0026】リセット入力端子105には、リセット信号RSTが与えられる。このリセット信号RSTは、内蔵されているCPU 112のみならず、分周器108や、シリアル/パラレル変換器107等を初期化するためにも用いられる。

【0027】データの入/出力は、双方向データ信号線I/Oを介して、シリアル/パラレル変換器107により行なわれる。シリアル/パラレル変換器107は、外部機器からシリアルデータで転送されてきたデータを、例えば8ビットのパラレルデータに変換する。

【0028】双方向データ信号線I/Oを介して入/出力されるシリアルデータは、「L」レベルのスタートビットが先頭にあり、その後LSBファーストの正論理 (又はMSBファーストの負論理、選択はICカード製造業者が行う) でビットデータが続き、偶数のパリティ1ビットが付加される。「L」レベルのスタートビットによりデータの先頭が検出され、それに続いて、データが送られる。そして、パリティによりエラーが検出される。このとき、パリティによりエラーが検出されれば、パリティビットに続く2クロックの間の特定時間に、受信側から「L」レベルが送出される。これにより、送信側では、エラーがあったことが分かる。エラーがあったことを分かると、送信側は、同じデータを再度送信す

(6)

特開2001-51903

る。

【0029】この方法は、ISO7816の半二重非同期通信プロトコルである。シリアル／パラレル変換器107は、これらの処理を経て、シリアルデータとパラレルデータとの変換処理を行なう。

【0030】RAM(Random Access Memory)109は、随時書き込み読み出しが可能であり、このRAM109は、CPU(Central Processing Unit)112が処理を行なっていく際に必要なデータを一時的に記憶したり、いくつかのデータ一時に蓄えておくために使用される。

【0031】EEPROM110は、内部だけで利用されるデータ、利用上更新しながら継続使用されるデータ等が記憶される。例えば、デジタルセルラー携帯端末では、短縮ダイアル、契約内容、ショートメッセージ、或いは通信を開始、維持するための制御データ等がEEPROM110に記憶される。

【0032】なお、ここでは、EEPROMを使用しているが、例えば、EEPROMの代わりに、フラッシュメモリを用いるようにしても良い。

【0033】ROM(Read Only Memory)111は、主に、CPU112が処理すべきプログラムが記憶されている。処理命令は、例えば、携帯端末を製造したり、利用するのに必要な公開された命令体系と、セキュリティ、例えばスクランブルキー発生部や、発行者又は管理者利用できないデータなどを操作するための非公開の管理用命令体系や暗証番号からなる。このように、非公開の管理用命令体系を用意することで、SIMセキュリティ機能がさらに高められている。

【0034】分周器108は、CPU112を作動させるためのクロックCLKから、双方向データ信号線I/O所定の伝送レートを使用してデータを送るためのクロックを得るものである。分周器108の分周比としては、例えば、GSM方式の携帯電話システムでは、1/372が用いられている。勿論、この分周比は、使用目的や使用状況により変更し得るものである。

【0035】CPU112は、外部からの命令に従って、SIM内部の処理を行うものである。この時、内部にアクセス権が或るか否か等が判断されて、処理が行なわれる。

【0036】データ用バス113は、CPU112が命令を実行する際に、命令をROM111から読み出したり、一時的にデータを記憶させるために、RAM109に随時読み出し／書き込みしたり、外部装置からの要求に基づいて、EEPROM110をアクセスしたりする際に、データを転送するのに用いられる。

【0037】このように、SIMの構成のICカードでは、EEPROM110には、短縮ダイアル、契約内容、ショートメッセージ、或いは通信を開始、維持するための制御データ等、内部だけで利用されるデータ、利

用上更新しながら継続使用されるデータ等が記憶される。また、ROM111には、例えば、携帯端末を製造したり、利用するのに必要な公開された命令体系と、セキュリティ、例えばスクランブルキー発生部や、発行者又は管理者利用できないデータなどを操作するための非公開の管理用命令体系からなる処理命令が記憶される。そして、入／出力されるデータは、CPU112により管理されている。このため、高いセキュリティ機能が保証されている。

【0038】2. メモリスティックの内部構成

次に、メモリスティックと呼ばれるメモリカードについて説明する。図2は、メモリスティックの内部構造を示すブロック図である。

【0039】メモリスティックには、電源端子201と、外部機器との接続のためのデータ入／出力端子202と、バスステートの入力端子203と、シリアルクロックの入力端子204と、挿抜検出用の検出端子205と、接地端子206とが配設される。

【0040】データ入／出力端子202により、双方向データ線DIOを介して、データが入／出力される。データ線DIOは、トランスマネージャー命令(TPC)という制御データやデータそのものを書き込んだり、読み出したりするためのものである。

【0041】バスステートの入力端子203には、バスステートBSが供給される。バスステートBSは、双方双方向データ信号線DIO上のデータに対するステータスを示している。例えば、データアクセスを行う前のTPCやデータそのものにより、そのステートを変化させることにより、メモリスティックの処理が実行される。

【0042】シリアルクロック端子204には、転送用クロックSCLKが供給される。転送クロックSCLKは、TPCやデータそのものを転送する際に発生される。転送クロックSCLKは、バスステートBSにより制御されている。

【0043】検出端子205は、外部装置がメモリスティックの着脱状態を検出するために使用される。メモリスティック内部では、この検出端子205は接地されており、外部装置によりブルアップ抵抗を介して電源に接続されている。したがって、検出端子205は、メモリスティック装着状態では「L」レベルになり、非装着時には「H」レベルになる。

【0044】接地端子206は、グランドVssに接続されている。

【0045】シリアル／パラレル変換器207は、書き込み時には、双方向データ信号DIOを通じ、転送クロックSCLKに同期して送られてきたシリアルデータを、8ビットのパラレルデータに変換する。制御用コマンドもデータも、ここでシリアルデータからパラレルデータに変換される。

【0046】一方、読み出し時は、メモリスティック内

(7)

特開2001-51903

部のフラッシュメモリ213に記憶されている8ビット毎のパラレルデータは、シリアル/パラレル変換器207でシリアルデータに変換され、双方向データ信号DIOを通じて、外部装置に出力される。

【0047】レジスタ208は、ステータスレジスタ、パラメータレジスタ、エキストラデータレジスタ等からなり、TPCによりメモリスティック内部のメモリのアクセス制御を行う。

【0048】ページバッファ209は、シリアル/パラメータ変換器207とフラッシュメモリ213間でデータ交換を行う際、一時的にデータを記憶するのに用いられる。

【0049】エラー検出コード発生部210は、例えば、CRC(Cyclic Redundancy Check)コード等のエラー検出コードを転送するデータ或いは転送されてくるデータに付加して、転送するデータ或いは転送されてくるデータの誤り検出を行なうものである。このようなエラー検出を行うことにより、データの信頼性が確保されている。

【0050】アトリビュートROM211は、メモリスティック内部の物理的情報を記憶するものである。このアトリビュートROM211の情報は、電源オン直後に読み出される。外部装置は、この情報を対応状況をチェックするために用いる。

【0051】フラッシュI/Fシーケンサ212は、レジスタ208に設定されているパラメータ等を基にして、ページバッファ209とフラッシュメモリ213間のデータの制御を行なっている。

【0052】フラッシュメモリ213は、例えばNAND型のメモリセルからなる不揮発性のメモリカードを用いたもので、ある容量のページ単位に区切られて、データの書き込み/読み出しが行われる。このフラッシュメモリ213の記憶容量は多種あるが、例えば、64MB程度まで計画されている。

【0053】このように、メモリスティックでは、フラッシュメモリ213により、例えば、64MB程度までのデータを記録できる。そして、このメモリスティックでは、シリアルの半二重同期データ転送方式を利用することで、20Mb/s程度のアクセス速度が確保できる。

【0054】3. スマートスティックの一例

3-1. スマートスティックの一例の構成

この発明は、図2に示したメモリスティックの構成のメモリカードを基本構成として、図1に示したSIMと呼ばれるICカードとの互換性を各信号線ベースで維持できるようにして、メモリスティックをインテリジェント化したものである。このようにインテリジェント化されたメモリスティックは、通常のメモリスティックとして使用できると共に、SIMと呼ばれるICカードと同様な機能を使うことができる。これにより、コンテンツの

データをダウンロードする際に、セキュリティが向上すると共に、電子マネー等により課金処理ができるようになる。以下、このようにインテリジェント化されたメモリスティックをスマートスティックと呼ぶことにする。

【0055】図3は、この発明が適用されたスマートスティックの内部構造の一例を示すものである。図3に示すように、このスマートスティックには、電源端子301と、プログラム用電源端子302と、双方向データ信号線I/Oの入出力端子302と、バステートの入力端子303と、転送クロック入力端子304と、挿抜検出用の検出端子306と、クロック入力端子306と、リセット入力端子307と、接地端子308が設けられる。

【0056】電源端子301は、作動電源Vccを外部から供給するためのものである。作動電源Vccの電圧は5V~3Vである。

【0057】入出力端子302は、双方向データ信号線I/Oにより実際にデータの入出力を行なうためのデータ入/出力端子である。双方向データ信号線I/Oには、SIMの双方向データ信号線(図1)又はメモリスティックの双方向データ信号線DIO(図2)と同様である。

【0058】バステートの入力端子303には、バステートBSが供給される。バステートBSは、双方双方向データ信号線上でパケット通信でデータを転送する際、データに対するステータスを示している。例えば、データアクセスを行う前のTPCやデータそのものにより、そのステートを変化させることにより、メモリスティックの処理が実行される。

【0059】なお、データの入出力には、バステートBSを使用しない非同期モードも可能である。この方式は、SIMで使用されているISO7816の半二重非同期通信プロトコルである。

【0060】転送クロック入力端子304には、転送用のシリアルクロックSCLKが供給される。この転送クロックSCLKは、パケット通信の状態で、バステートBSによりクロック発生が制御される。半二重非同期通信プロトコルでは、転送クロックSCLKは使用されない。

【0061】検出端子305は、外部装置がスマートスティックの着脱状態を検出するために使用される。スマートスティック内部では、この検出端子305は接地されており、外部装置によりブループラット抵抗を介して電源に接続されている。したがって、検出端子305は、メモリスティック装着状態では「L」レベルになり、非装着時には「H」レベルになる。

【0062】クロック入力端子306には、作動クロックCLKが供給される。この作動クロックは、CPU306を作動させるために、CPU316に供給される。

(8)

特開2001-51903

【0063】リセット入力端子307には、リセット信号RSTが供給される。このリセット信号RSTにより、内蔵されているCPU316が初期化されると共に、シリアル/パラレル変換器309や、制御用のレジスタ310、スクランブル311a等が初期化される。

【0064】接地端子308は、グランドVssに接続されている。

【0065】シリアル/パラレル変換器309は、外部装置とのデータの交換を行なえるように、シリアルデータとパラレルデータとの変換を行なっている。外部装置との間では、双方向データ通信線I/Oを介して、シリアルデータで転送が行なわれ、内部では、8ビットのパラレルデータで処理が行われる。シリアル/パラレル変換器309は、シリアルデータと、8ビットのパラレルデータとの変換処理を行なっている。

【0066】レジスタ310は、ステータスレジスタとコントロルレジスタからなり、CPU316がシリアル/パラメータ変換器309の監視と制御を行なうために用いられる。

【0067】スクランブル311aは、データを暗号化して記憶させることができるようとするものである。暗号化してデータを記憶させるのは、記憶されているデータの保護を図るためである。例えば、何かの方法でフラッシュメモリ315の部分だけを取り外すことができたとすると、悪意のある試みとして、何人かにより、フラッシュメモリ315の部分だけが取り出され、フラッシュメモリ315の内容が読み取られ、そこに書かれているコンテンツや個人情報が盗まれる危険性がある。フラッシュメモリ315にデータを記憶させる際に、データを暗号化しておけば、たとえフラッシュメモリ315の部分だけが取り出され、その内容が読み取られたとしても、コンテンツや個人情報については保護できる。スクランブル311aの暗号化のアルゴリズムについては、後に、詳述する。

【0068】エラー検出コード発生部311bは、例えば、CRC (Cyclic Redundancy Check) コード等のエラー検出コードを転送するデータ或いは転送されてくるデータに付加して、転送するデータ或いは転送されてくるデータの誤り検出を行なうものである。このようなエラー検出を行うことにより、データの信頼性が確保されている。

【0069】ページバッファ312は、予め決められたデータ容量を一時的に記憶し、シリアル/パラメータ変換器309とフラッシュメモリ315間でデータ交換を行う際、一時的にデータを記憶するのに用いられる。

【0070】RAM313は、CPU316が外部装置から与えられた命令を処理する際に、一時的に発生する演算結果、パラメータ等を記憶するために用いられる。

【0071】ROM314は、主に、CPU316が処理すべきプログラムが記憶されている。処理命令は、例

えば、携帯端末を製造したり、利用するのに必要な公開された命令体系と、セキュリティ、例えばスクランブルキー発生部や、発行者又は管理者以外は利用できないデータなどを操作するための非公開の管理用命令体系や暗証番号からなる。このように、非公開の管理用命令体系を用意することで、セキュリティ機能がさらに高められている。

【0072】また、ROM314には、外部から見えるファイルと、管理用及び暗号に関係した処理にのみ使用される管理用命令体系以外ではアクセスできない隠されたファイル等を操作するためのプログラムが記憶されている。

【0073】フラッシュメモリ315は、例えばNAND型のメモリセルからなる不揮発性のメモリカードを用いたものである。メモリフラッシュメモリ315には、見えるファイルも管理用の外部から見えないファイルも、後に説明するディレクトリデスクリプションやファイルデスクリプションに従って、フラッシュメモリ315に記憶される。

【0074】CPU316は、外部装置から転送された命令を、読み出し専用メモリ314から必要なプログラムを随時読み出して処理を行う。

【0075】3-2. 外部装置とスマートスティックとのセッション

次に、外部装置であるホストコンピュータが、上述のようにインテリジェント化されたメモリスティック（スマートスティック）をどのように制御するかについて説明する。

【0076】図4は、外部装置が上述のスマートスティックを制御する際のセッションを示すもので、これは、従来のGSM方式の携帯電話におけるSIMの制御を行なうのに適用したものである。

【0077】先ず、スマートスティックを起動するためには、ホストコンピュータは、電源Vcc、クロックCLK、リセット信号RSTの供給を行なう（ステップST1）。送る順番は、電源電圧Vcc、プログラム電源Vpp（内部で供給する場合には不要、また外部から供給する場合VCCと同時にあっても良い）、クロックCLK、リセット信号RSTの順である。

【0078】リセット信号RSTを「L」レベルから「H」レベルに状態変化させると、スマートスティックは動作状態に入る（ステップST2）。スマートスティックの内部では、ホストコンピュータから命令を受け取るための初期化が行なわれる。

【0079】次に、ホストコンピュータはスマートスティックに、実行命令コマンドを送る（ステップST3）。この実行命令コマンドは、例えばいくつかのバイトで構成されており、最初のバイトは応用分野毎にコードが予め決められている。このことにより、マルチファンクションの動作が可能になる。次のバイトは処理命令

(9)

特開2001-51903

コードを表し、それに続くバイトは命令を実行する際に必要なパラメータなどからなる。

【0080】スマートスティックは、ホストコンピュータから実行命令コマンドを受け取り、そのコマンドを確認できると、ホストコンピュータにアクノリッジを返す（ステップST4）。

【0081】次に、ホストコンピュータがコマンドを送り、スマートスティックからアクノリッジが返されると、ホストコンピュータとスマートスティックとの間でデータのやり取りが可能となる。そして、実行命令コマンドの内容に従って、ホストコンピュータからスマートスティックに向かって、或いはスマートスティックからホストコンピュータに向かって、データが転送される（ステップST5）。

【0082】最後に、スマートスティックは、実行命令終了状況をホストコンピュータへ知らせるために、2バイトのステータワードをホストコンピュータに送出する（ステップST6）。

【0083】その後の通常のセッションでは、ホストコンピュータからスマートスティックへの実行命令コマンドの送出（ステップST3）から、スマートスティックからホストコンピュータへのステータスワードの送出（ステップST6）までが1回のアクセスとして、セッションが繰り返される。

【0084】3-3. 暗号化について

図3に示したように、この発明が適用されたスマートスティックでは、フラッシュメモリ315に、データを暗号化して記憶させることができる。このときの暗号化キー生成について説明する。

【0085】図5は、暗号化キーの生成処理を示すものである。図5において、暗号化キー演算回路403は、2つのパラメータから暗号化キーを発生するアルゴリズムの演算を行なうものである。暗号化キー演算回路403は、図3におけるスクランブル311aにハードウェアとして設けられる。

【0086】暗号化キー演算回路403には、入力端子401及び402から2つのパラメータが与えられる。一方のパラメータとしては、ユーザーの暗証番号（PIN: Personal ID Number）が使用される。なお、この暗号化キー生成用のパラメータとしては、暗証番号でなくともよく、例えば、カード発行時に会社に登録されている加入者番号や、ある特定グループ内で使用されるコードであっても良い。

【0087】他方のパラメータとしては、暗号情報Kiが用いられる。前述したように、スマートスティックの命令体系には、公開されている命令体系と、非公開の命令体系とがあり、非公開の命令体系は、発行者又は管理者以外利用できない。暗号情報Kiは、非公開の命令体を使わないとアクセスできないように設定されている。

【0088】暗号化キー演算回路403で、ユーザーのP

INと暗号情報Kiをパラメータとして、暗号化キーが生成される。そして、暗号化キー演算回路403により生成された暗号化キーKcが出力端子404から出力される。

【0089】上述のようにして生成された暗号化キーKcを使用して、図6に示すような暗号化処理回路により、暗号化処理が行なわれる。

【0090】図6において、暗号化アルゴリズム演算回路452は、所定の暗号化アルゴリズムにより、入力データを暗号化して出力するものである。暗号化アルゴリズム演算回路452は、図3におけるスクランブル311aにハードウェアで構成されている。

【0091】暗号化アルゴリズム演算回路452には、入力端子451から暗号化キーKdが供給される。この暗号化キーKdは、図5の暗号化生成例で示した演算結果として得られた暗号化キーKcに、変化するパラメータ（ここでは、ページモードアクセスする際のページ番号）を加えた値である。

【0092】このように、生成された暗号化キーKcにある基準からの相対番号を加えた値を暗号化キーとしているのは、セキュリティを強化するためである。暗号化キーKcが変化しない場合には、暗号化されたデータと平文とを比較によりスクランブルアルゴリズムを予測して暗号を解読するという可能性が残され、セキュリティ上問題となる可能性がある。

【0093】なお、ここでは、暗号化キーKcに対して変化するパラメータとしてページモードアクセスする際のページ番号を用いているが、この変化するパラメータは、入出力時に一致するものであれば何でも良く、例えば、電子的書き換え可能な不揮発性メモリ、フラッシュメモリのデータが格納される最初のアドレスを基準にした相対値でも良い。

【0094】暗号化アルゴリズム演算回路452には、入力端子453から、平文のデータ（暗号化前のデータ）が与えられる。この平文のデータは、外部装置からシリアルデータとして送られてきた後、シリアル/パラレル変換器309で8ビット変換されたデータを意味している。暗号化アルゴリズム演算回路452で、この入力データに対して、入力端子451からの暗号化キーKd（暗号化キーKc+ページ番号）を用いて、暗号化が行なわれる。

【0095】暗号化アルゴリズム演算回路452により暗号化されたデータが出力端子454から出力される。この暗号化されたデータがフラッシュメモリ315（図3）に記憶される。

【0096】このように、スクランブル311a（図3）にハードウェアで構成された暗号化アルゴリズム演算回路452には、平文のデータと、暗号化キー（暗号化キーKc+ページ番号）とが供給され、暗号化アルゴリズム演算回路452により、所定の暗号化アルゴリズ

(10)

特開2001-51903

ムにより、暗号化データが生成される。この暗号化されたデータが出力端子454から出力され、最終的に、フラッシュメモリ315(図3)に記憶される。

【0097】なお、上述の例では、外部装置から入力された平文のデータを暗号化してフラッシュメモリ315に記憶させる際の処理について説明したが、フラッシュメモリ315に記憶されているデータを読み出し、暗号化されたデータを解読して平文のデータに戻して、外部装置に出力する際の処理については、上述の手順と逆の手順で行なえば良い。

【0098】また、フラッシュメモリ315にデータを記憶する場合に、常に、データを暗号化する必要はない。必要に応じて、データを暗号化せず、平文データのままフラッシュメモリ315に記憶させ、フラッシュメモリ315から平文で出力させることも可能である。また、これとは反対に、フラッシュメモリ315にデータを暗号化して記憶させ、この暗号化されたデータが記憶されているフラッシュメモリ315から、暗号解読しないまま、暗号化されたデータを外部装置に出力することも可能である。

【0.0.9.9】3-4. ファイル構成について

次に、フラッシュメモリ315上に展開されるレクトリやファイルの構成について説明する。このファイル展開の方式は、GSM方式の携帯電話で使用されているSIMのファイル管理方式に改良を加えたものである。

【0100】図7は、ディレクトリの仕様を示すものである。ディレクトリのデスクリプションは、メインディレクトリと、メインディレクトリの下に構成されるサブディレクトリの情報を提供するものである。メインディレクトリのデスクリプションと、サブディレクトリのデスクリプションは同様である。

【0101】この発明が適用されたスマートスティックをマルチファンクションで使用する場合、例えば、通信用のメインディレクトリ、電子出版用のメインディレクトリ、ゲームのダウンロード用のメインディレクトリ、或いは最終使用者が自由に利用できるディレクトリ等に分けて使用することが想定される。このような場合、それぞれの目的に応じてセキュリティの設定条件が異なるため、それぞれで管理情報を有することになる。

【0102】図7は、ディレクトリのデスクリプションを示すものである。ディレクトリのデスクリプションは、メインディレクトリ又はサブディレクトリの容量、ファイル数、セキュリティ用の暗証番号機能が提供されているか、ロック停止が可能かどうか等の情報が含まれている。管理用の隠されたディレクトリ以外は、この情報は外部装置から読み出すことが可能で、メモリスティックを制御するためにも使用される。

【0103】ディレクトリのデスクリプションは、共通の仕様(図7A)と、各アプリケーション用の仕様(図7B)に大別される。

【0104】先ず、図7Aに示す共通の仕様について説明する。共通仕様では、アプリケーションによらず、全てに共通したフォーマットでコーディングされる。共通仕様のバイトB1～バイトB4は、残存有効メモリ量を示しており、スマートスティック全体で利用できる残りのメモリ量を示す。

【0105】バイトB5～バイトB20は、ディレクトリID及びタグで、2バイトのコードと残りは例えばASCIIの平文タイトルなどに使用される。ディレクトリID及びタグは、ここでは例として16バイトを設定しているが、勿論、より多くのバイト数を割り当ててもかまわない。

【0106】バイトB21はディレクトリタイプで、ディレクトリ或いはファイルの識別をするためのデータをコーディングしている。図7Cは、バイトB21のコーディング例を示している。例えば、マルチファンクションで使用する場合、アプリケーション毎のメインディレクトリは「01h(hは16進数を示す)」、その下のサブディレクトリは「02h」、データファイルを表す場合は「04h」にコーディングされる。

【0107】バイトB22～バイトB27はタイムスタンプである。このタイムスタンプは、GSM方式の携帯電話におけるSIMには用いられていない情報である。例えばフロッピーディスクやハードディスク等で新たにディレクトリを作成した場合には、必ずタイムスタンプが規約される。このタイムスタンプは、そのことを想定して設けたものである。また、発行者が時限付きで使用を許諾するようなソフトウェアの販売や電子出版にも、タイムスタンプは使用可能である。例えば、タイムスタンプを参考にして期限切り替えられると、内容を読み出せないするという操作も可能である。ここでは、時刻分単位までの記入例だが、勿論、秒単位であっても良い。

【0108】バイトB28～B29は、将来の拡張性を鑑みて、リザーブされている。

【0109】バイトB30は、次に続くアプリケーション用のファイルのデータ長で、各アプリケーション用の仕様のサイズで、どこまでがディレクトリデスクリプションかを示すために用いられる。サブディレクトリデスクリプションやデータファイルがこれに連続してアプリケーション可能のようにし、メモリの有効活用をする。

【0110】次に、図7Bに示す各アプリケーション毎の仕様について説明する。図7Bにおいて、バイトB31はディレクトリキャラクタリストリクエストである。図7Dがそのコーディング例を示している。例えば、このスマートスティックに供給されているCPU用の作動クロックの停止が可能か否か、停止可能な場合の状態が「H」レベル或いは「L」レベルで、停止するのかどちらでも良いのかがコーディングされている。また、停止したときの状態により消費電流が変わる場合もあり、携

(11)

特開2001-51903

端末等では少しでもこれを少なくできるように配慮している。

【0111】また、ディレクトリキャラクタリスティクスのビットB₁₈は、PIN1が有効であるか無効であるかを示している。PIN1は、主に使用者の正当性を確認するための暗証番号が設定されており、この状態が簡単にチェックできる。

【0112】バイトB32～バイトB33は、サブディレクトリ数を示し、例えば、マルチファンクションで使用されている場合に、アプリケーション別に設定されるメインディレクトリの下に、サブディレクトリがいくつ存在しているかをコーディングしている。

【0113】バイトB34～バイトB35は、ファイル数を示し、例えば、マルチファンクションで使用される場合に、アプリケーション別に設定されるメインディレクトリの下とサブディレクトリの下に、ファイルがいくつ存在しているかをコーディングしている。

【0114】バイトB36は、PIN、アンブロッキングPIN、アドミニストレイティブコード数、暗証番号、暗証番号がブロックされている場合の解除番号、或いは管理用の特別なコードがいくつ設定されているかを示している。例えば、PINが2種類設定されており、更に一般的には公開されず利用できない管理者用のアドミニストレーティブコードが2種類設定されていたとすると、「4(h)」という値にコーディングされる。

【0115】バイトB37は、将来の拡張性のためにリザーブされている。

【0116】バイトB38は、PIN1ステータスである。図7Eに、セキュリティステータスのコーディングが示されている。例えば、PIN1が設定されていたなら、ビットB₁₈が「1」にコーディングされ、更に、連続誤入力カウンタが「3」に設定されていたなら「83(h)」というコードになる。この場合、連続してPIN1の暗証番号を誤ると、PIN誤入力カウンタは「0」になり、使用者はこれ以上PIN1の検証をすることがでなくなる。この状態をPIN1がブロックされているという。また、PIN1の検証が正しく行なわれた場合は、PIN誤入力カウンタの値は初期値「3」にリセットされる。

【0117】バイトB39は、アンブロッキングPIN1ステータスを示している。図7Eに、セキュリティステータスのコーディングが示されている。例えば、PIN1が設定されていたなら、それと一対をなすこのアンブロッキングPIN1ステータスのビットB₁₈が

「1」にコーディングされる。PIN1ステータスの誤入力カウンタが「0」で、PIN1がブロックされた場合に、これを解除するために別に用意された暗証番号PUK(Unlocking Personal Key)であり、この状態を示しているのが、アンブロッキングPIN1ステータス

である。

【0118】このアンブロッキングPIN1ステータスも、例えば、連続誤入力カウンタが「10」に設定されていたなら、「8A(h)」というコードとなる。この場合、連続して10回この暗証番号PUK1を誤ると、アンブロッキングPIN1誤入力カウンタは「0」になり、使用者はこれ以上PIN1のブロック解除を行うための暗証番号PUK1の検証ができなくなる。この状態では、最早、発行者或いは管理者が使用する管理命令体系を使用して復元するしか手段がなくなる。このような点も、セキュリティを高めている。また、PIN1ブロック解除用の暗証番号PUK1の検証が正しく行なわれた場合は、PUK1誤入力カウンタの値は初期値「10」にリセットされ、使用者は新たにPIN1を設定する。

【0119】バイトB40はPIN2ステータス、バイトB41はアンブロッキングPIN2ステータスを示している。PIN2ステータス、アンブロッキングPIN2ステータスは、PIN1ステータス及びアンブロッキングPIN1ステータスと同様である。

【0120】バイトB42～B48はアドミニストレーティブマネージメントユーズで、例えば、端末製造業者等には公開されていない命令体系を使用する場合に利用される。

【0121】次に、データファイルのアクティブ等を直接管理するための情報が記述しているファイルデスクリプションについて説明する。

【0122】図8は、ファイルデスクリプションを示すものである。このファイルデスクリプションは、共通仕様(図8A)と、各アプリケーション用の仕様(図8B)とに分けることができる。

【0123】図8Aは、共通仕様を示している。図8Aにおいて、バイトB1～バイトB4は、ファイルサイズを示している。

【0124】バイトB5～バイトB20は、ファイルID及びタグで、2バイトのコードと残りは例えばASC IIの平文タイトルなどに使用する。ファイルID及びタグは、ここでは例として16バイトを設定しているが、勿論もっと多く割り当ててもかまわない。

【0125】バイトB21はファイルタイプである。図8Cはコーディング例を示している。データファイルの場合には、「04(h)」にコーディングされる。

【0126】バイトB22～バイトB27はタイムスタンプで、GSM方式の携帯電話におけるSIMにはない情報である。例えばフロッピー(登録商標)ディスクやハードディスク等で新たにディレクトリを作成した場合には、必ずタイムスタンプが規約される。このタイムスタンプは、そのことを想定して設けたものである。また、発行者が時限付きで使用を許諾するようなソフトウェアの販売や電子出版にも、タイムスタンプは使用可能

(12)

特開2001-51903

である。例えば、タイムスタンプを参考にして期限切り換えると、内容を読み出させないするという操作も可能である。ここでは、時刻分単位までの記入例だが、勿論、秒単位であっても良い。

【0127】バイトB28はモードを示している。図8Dはそのコーディング例を示す。例えば、課金情報などの単位を一定時間毎に1命令でインクリメント可能なファイル構造を有するファイルで、この命令が実行可能か否かを示している。例えば、課金情報がもうインクリメントできない状態までカウントアップされたら、このスマートスティックが利用できないなどの管理に利用できる。

【0128】バイトB29～バイトB32はアクセスコンディションを示ししている。図8Eはそのコーディング例を示す。各バイト毎に対応した命令を実行するときに、満たされている必要のあるセキュリティ条件を設定する。

【0129】ここでバイトB32は、スマートスティックのアクセス条件を示している。図8Fはコーディング例である。バイトB32のビットB_it1～B_it4は、スクランブルを使用する際に、また、ビットB_it5～ビットB_it8は、コピーに関連してたアクセスをする際に、満たさなければならない条件で、そのコーディングがアクセスコンディションで示される。

【0130】アクセスコンディションコードが「0(h)」のときには、常にアクセス可能である。「1(h)」のときには、PIN1の検証が正常に終了していた場合にアクセスが可能である。「2(h)」のときには、PIN2の検証が正常に終了した場合にアクセスが可能である。「3(h)」は、将来の拡張のためにリザーブされている。「4(h)」は非公開の管理用のアクセス条件を満たしたときに利用できることを意味している。F(h)はアクセスが不可能であることを示している。例えば、バイトB32が「01(h)」とコーディングされていたら、スクランブルはPIN1の検証が正常終了した場合には利用でき、コピーは自由に可能であることを示している。

【0131】バイトB33はファイルステータスであり、このファイルの状態を示している。図8Gはコーディング例である。例えば、ビットB_it1はこのファイルが利用できるか否かを示す。また、ビットB_it2は記録されているデータがスクランブルされているか否かを示す。

【0132】バイトB34は、次に続くアプリケーション用のファイルデータ長で、各アプリケーション用の仕様のサイズで、どこまでがティレクトリデスクリプションかを示すために用いられる。サブディレクトリデスクリプションやデータファイルがこれに連続して位置できるようにして、メモリの有効活用がなされる。

【0133】次に、各アプリケーション用の仕様の内容

について説明する。図8Bは各アプリケーション用の仕様を示すものである。図8Bにおいて、バイトB35はストラクチャオブデータファイルで、ファイルの論理構造を示している。

【0134】ストラクチャオブデータファイルが「00(h)」にコーディングされた場合には、通常のメモリと同じように、ある容量のデータがそのまま記憶される。「01(h)」にコーディングされた場合には、ある決まったフォーマットのデータがグループ化されて記録されていく。例えば、短縮ダイアルの1件分を50バイトとした場合、この1件分をレコードと称してまとめて扱い、例えば、100レコードとして50バイトのメモリが確保されることになる。「03(h)」にコーディングされた場合は、「02(h)」のリニアフィックスと同レコードのフォーマットを有するが、このレコードの順番を順次入れ換えることができる。これは、優先順位を変更して、例えば、最初のレコードに持ってくるというような利用が可能である。つまり、受信に第1レコード、第2レコードから始まり、第nレコードまでとすると、このレコードの順番を入れ替え、第1レコードを第nレコードにし、それまで第2レコードであったレコードを新たに第1レコードとする方法である。

【0135】バイトB36～バイトB37は、レングスオブレコードで、1つのレコードのメモリサイズを示している。ファイルサイズとこのレングオブレコードから、いくつのレコードが使用できるか算出が可能である。

【0136】3-5. アクセス処理について
以下、この発明が適用されたスマートスティックのアクセス処理について、いくつかの命令処理を例にとって、フローチャートを使用して説明する。

【0137】図9は、この発明が適用されたスマートスティックの基本的動作を示している。図9において、パワーオンで、外部装置から電源を供給する。この時、必要ならば、フラッシュメモリのプログラ電源V_{pp}を同時に供給する（ステップS11）。

【0138】次に、CPU作動クロックの供給CLKを外部装置から供給する（ステップS12）。その後、リセット信号が「L」レベルから「H」レベルに変化して、CPUが作動状態に入るか否かの判断を行なう（ステップS13）。

【0139】外部装置がスマートスティックを起動させていない場合には、リセット信号は「L」レベルから「H」レベルに変化しない。このときには、パワーオフ判断（ステップS20）に進む。

【0140】一方、外部装置がスマートスティックを起動した場合には、リセット信号は「L」レベルから「H」レベルに変化する。このときには、初期化設定に移り（ステップS14）、外部装置からのコマンド受領、データ交換の準備をする。

(13)

特開2001-51903

【0141】次に、外部装置からコマンド待ち状態で、コマンドが入力されるか否かが判断される（ステップS15）。もし、コマンドの入力がなければ、リセット信号RSTのチェックに移る（ステップS19）。

【0142】一方、ステップS15で、コマンド入力があったら、そのコマンドを受付たことを外部装置に回答するために、アクノリッジの出力処理を行なう（ステップS16）。続いて、そのコマンドに対応処理として、データの出力処理又は入力処理のデータ処理を行なう（ステップS17）。そして、その処理の終了状況を外部装置に知られるために、ステータスワードを出力する（ステップS18）。

【0143】これが終了したら、リセット信号をチェックするために、リセット信号判断を行ない（ステップS19）、リセット信号RSTが「H」レベルなら、再びコマンドを受け付けるために、パワーオフ判断を行う（ステップS20）。

【0144】ここで、パワーオフであれば、リセットチェックに戻り（ステップS13）、パワーオフであれば全ての機能を停止する処理に移り、処理を完了する（ステップS21）。

【0145】次に、セキュリティに関係した暗証番号の処理について、図10のフローチャートを参照して説明する。

【0146】なお、ディレクトリデスクリプションで記述したPIN1、PIN2、PUK1、PUK2の扱いは、誤り入力数が異なるだけで処理についてはと同様であるから、一括して説明する。

【0147】図10において、PIN入力があったときに、スタートS31から処理を開始する。

【0148】次に、PIN1、PIN2、PUK1、PUK2の何れかを設定するPINモードの設定を行う（ステップS32）。この設定に従って、該当するPINが初期化されているか否かの判断を行なう（ステップS33）。

【0149】初期化されていない場合には、初期化されていないことを示すステータスを、図9メインルーチンフローチャートの中のステータスワードアウトプット処理（ステップ18）にて、外部装置に出力し（ステップS40）、処理を終了する（ステップS45）。

【0150】初期化されていたなら、PINがブロックされているか否かをチェックするために、誤入力カウンタの値が「0」か否かを判断する。もし、誤入力カウンタが「0」であったならば、外部装置にブロックされていることを示すステータスを出力する（ステップS44）。

【0151】誤入力カウンタが「0」でなかったならば、該当するPINがブロックされていないので、次に、該当するPINの検証機能が必要かのPINイネーブル判断処理がなされる（ステップS35）。該当する

PINの検証機能が不要に設定されている場合には、PINがディスイネーブルであることを示すステータスを外部装置に出力する（ステップS41）。

【0152】PINの検証機能が必要な場合には、予め記憶してある該当PINの内容と、入力されたPINの比較を行なう（ステップS36）。

【0153】この結果、予め記憶されているPINと、入力されたPINとが一致したか否かを判断する（ステップS37）。もし、入力されたPINが誤りならば、誤入力カウンタを更新するための誤入力カウンタのデクリメント処理を行い（ステップS42）、更に誤ったPINの入力があったことを外部装置に知らせるために、PINが誤っていることを示すステータスを出力して（ステップS43）、処理を終了する（ステップS45）。

【0154】予め記憶してあるPINと入力されたPINが一致した場合には、誤入力カウンタを初期化し、それに加えて関連するPINの誤入力カウンタも同時に初期化可する（ステップS38）。そして、通常終了コマンドを示すステータスを出力して（ステップS39）、処理を終了する（ステップS45）。

【0155】次に、ファイルアクセスの処理について、ファイル更新処理を例にして説明する。なお、他のコマンドの処理も同様に行なわれる。

【0156】図11は、ファイル更新のフローチャートを示すものである。まず、外部装置から更新コマンドが入力され、処理が起動される（ステップS51）。

【0157】次に、ファイルデスクリプション（図8）中で、更新の条件がコーディングされているバイトB29のビットB1t1～B1t4（図8F参照）を参照するために、更新条件の設定をCPUが行う（ステップS52）。次に、ファイルデスクリプション中のアクセスコンディションコードのどれに該当するかを順次チェックする。

【0158】最初にファイルのアクセスが禁止されているか否かの判断を行なう（ステップS53）。もし、アクセスが禁止されているならば、外部装置に条件が不十分である旨を通知するアクセス条件が満足しないことを示すステータスを出力する（ステップS69）。

【0159】ステップS53で、もし、アクセスが禁止されていなければ、管理上のコード検証に該当するか否かを判断する（ステップS54）。もし、該当するなら、検証判断（ステップS57）に進む。

【0160】もし、管理上のコードに該当しないならば、PIN1での検証に該当するか否かを判断する（ステップS55）。該当するなら、検証判断（ステップS57）へ進む。

【0161】該当しない場合は、図8に示したファイルデスクリプション中のアクセスコンディションコードの検証不要コード（ALW）に該当するので、ステップS

(14)

特開2001-51903

58に進み、スクランブル条件の判断設定を行なう。

【0162】ステップS54、ステップS55及びステップS56での判断の結果、いずれかに該当すると判断された場合には、該当するPIN或いはコードの検証が済んでいるか否かの判断を行なう(ステップS57)。

【0163】該当するPIN或いはコードの検証が済んでいない場合は、外部装置にPINの検証が済んでいないことを示すステータスを出力する(ステップS68)。

【0164】次に、図8に示したファイルデスクリプション中のアクセスコンディションコードのどれに該当するかを順次チェックする。

【0165】最初に、管理上のコード検証に該当するか否かを判断する(ステップS59)。もし、管理上のコードに該当しなければ、PIN1での検証に該当かを判断する(ステップS60)。PIN1での検証に該当しないなら、PIN2での検証に該当するかを判断する(ステップS61)。

該当しない場合には、ファイルデスクリプション中のアクセスコンディションの不使用コード(NEV)に該当するので、スクランブルを使用しない設定をして処理を行う(ステップS67)。

【0166】一方、ステップS59、S60、S61の何れかで、条件に該当すると判断された場合には、該当するPIN或いはコードの検証が済んでいるか否かの判断を行なう(ステップS62)。該当するPIN或いはコードの検証が済んでいない場合には、外部装置に、PINの検証は不成功であることを示すステータスを出力する(ステップS68)。

【0167】ステップS62で、検証が済んでいると判断された場合には、暗号化キーKcを参照するために、暗号化キーの計算処理を実行する(ステップS63)。ここで得られた暗号化キーKcを使って、暗号キー(Kc+ページ番号)により暗号化するような、スクランブルモードとなるように、スクランブルモードに設定する(ステップS64)。このとき、例えば、複合暗号キーの一部をなすページ番号は、ハードウェアから直接入力してもかまわない。

【0168】こうして、事前にスクランブルを使用するか否かを選択された後、実際にデータの更新が実行され(ステップS65)、全てのデータの更新が完了した時点で、外部装置に正常終了を知らせるステータスを出力して(ステップS66)、終了となる(ステップS70)。

【0169】4. スマートスティックの他の例

次に、この発明が適用されたスマートスティックの他の例について説明する。図12は、この発明が適用されたスマートスティックの他の例の内部構造を示すものである。

【0170】前述の図3に示したスマートスティックでは、シリアル/パラレル変換器309に対する転送用ク

ロックSCLKをクロック入力端子304から供給するようしているが、この例では、CPUの作動クロックを分周器320で分周して、転送用のクロックSCLKとしている。その他の構成については、前述の図3に示した例と同様である。

【0171】このように、転送クロックSCLKを作動クロックCLKを分周して形成することにより、クロックに係わる信号線が1つ不要になり、單一クロックでの動作が可能となる。これにより、外部装置の負担が軽減される。

【0172】一方、この例では、転送クロックSCLKは作動クロックCLKの関係が分周器320の分周比で決められるため、転送クロックSCLK及び作動クロックCLKの周波数を任意に決められなくなる。また、転送クロックSCLKと作動クロックCLKとを独立して止められなくなる。

【0173】このことは、とりもなおさず、ISO7816に規定されている半二重非同期通信プロトコルに対応した動作で、特に、負の要因とはならない。むしろ、GSM等で仕様されているSIMの代替えとしての可能性が増すことになる。

【0174】また、この例では、CPUが処理を行なっていない場合、適正な手順で作動クロックを停止させることができる。この作動クロック或いは転送クロックの停止機能は、携帯端末において、バッテリ駆動されるという観点から、消費電力の低減が必須となり、有効な手段と言える。

【0175】なお、この発明が適用されたスマートスティックは、CPUを内蔵しているため、コンテンツデータの記憶用としてばかりでなく、種々の分野に応用可能である。例えば、外部記憶ばかりでなく、パーソナルコンピュータのコプロセッサとしても利用できる。

【0176】

【発明の効果】この発明によれば、メモリスティックの構成のメモリカードに、CPUと、暗号化回路が設けられる。そして、入出力されるデータは、暗号化されて、フラッシュメモリに記憶される。また、メモリスティックをアクセスするための命令体系には、公開された命令体系と非公開の命令体系とを有している。フラッシュメモリに記憶されるファイルデータは、各ファイルデータ毎に、アクセス制限、コピーガード情報、及びアクセス時の暗号化、暗証番号を選択的に設定できる。これらのファイルデータは、隠されたデータファイルを含むデータファイルが処理を管理している。また、ファイルデータにはアクセス権が設定され、アクセス権に従って、ファイルデータの読み出し及び書き込みのアクセスが制限される。このように、データが暗号化されてフラッシュメモリに記憶されるため、記憶されるデータのセキュリティが強化される。

【図面の簡単な説明】

(15)

特開2001-51903

【図1】SIMの説明に用いるブロック図である。

【図2】メモリスティックの説明に用いるブロック図である。

【図3】この発明が適用されたメモリカードの一例のブロック図である。

【図4】この発明が適用されたメモリカードの一例の説明に用いる略線図である。

【図5】この発明が適用されたメモリカードの一例における暗号化の説明に用いるブロック図である。

【図6】この発明が適用されたメモリカードの一例における暗号化の説明に用いるブロック図である。

【図7】この発明が適用されたメモリカードの一例におけるディレクトリの説明に用いる略線図である。

【図8】この発明が適用されたメモリカードの一例にお

けるファイルの説明に用いる略線図である。

【図9】この発明が適用されたメモリカードの一例の説明に用いるフローチャートである。

【図10】この発明が適用されたメモリカードの一例の説明に用いるフローチャートである。

【図11】この発明が適用されたメモリカードの一例の説明に用いるフローチャートである。

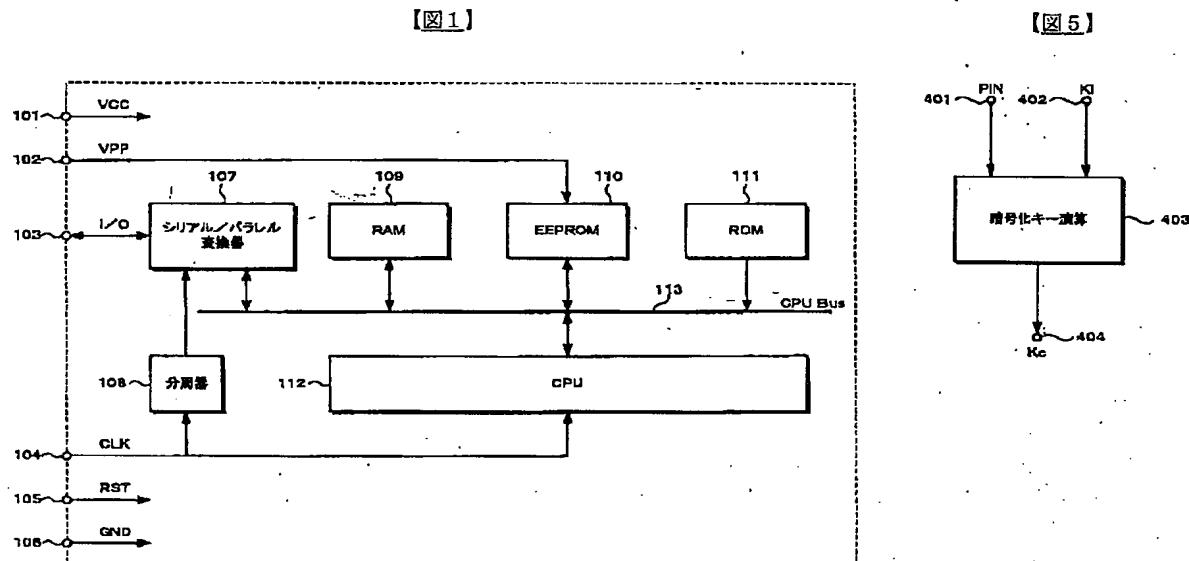
【図12】この発明が適用されたメモリカードの他の例のブロック図である。

【符号の説明】

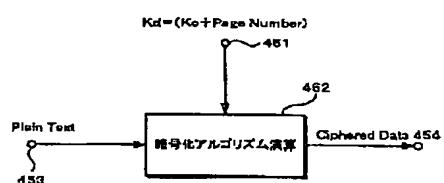
309...シリアル/パラレル変換器、310...

レジスタ、315...フラッシュメモリ、316...

・CPU



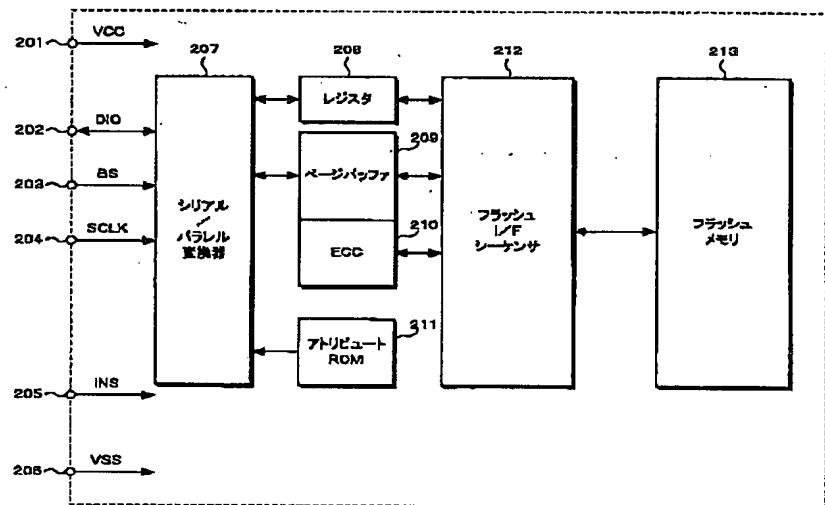
【図6】



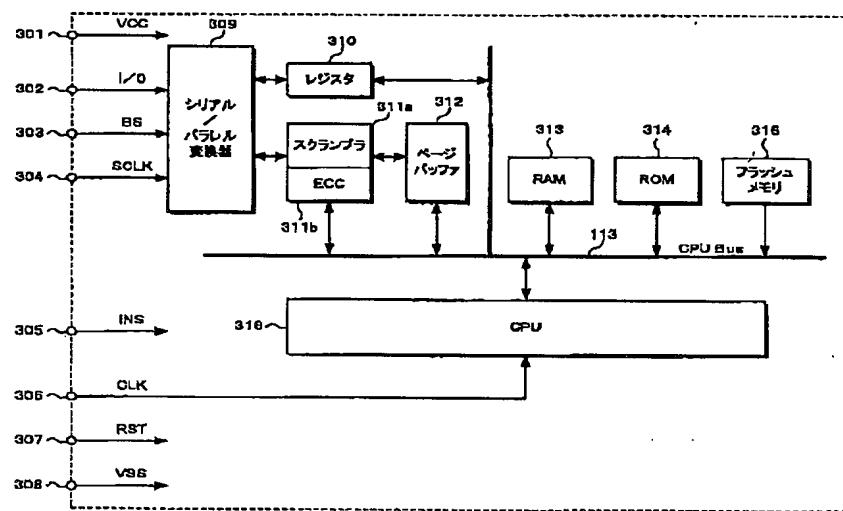
(16)

特開2001-51903

【図2】



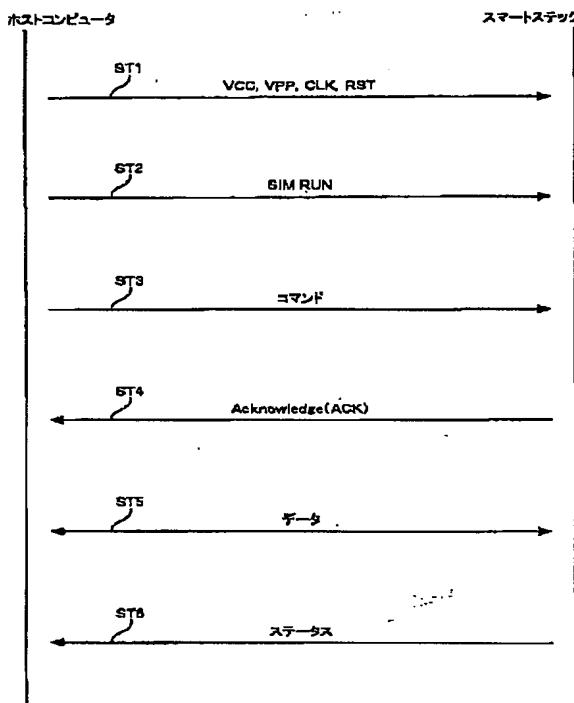
【図3】



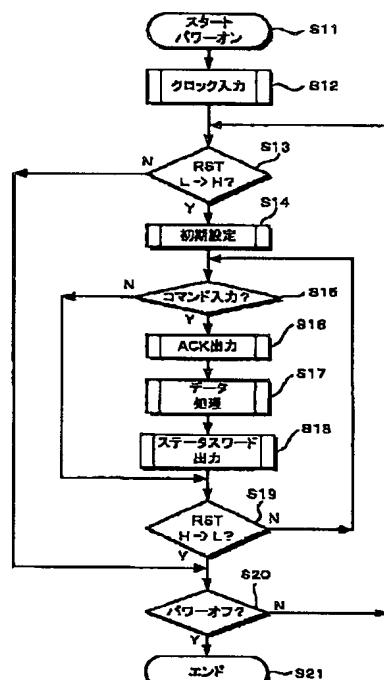
(17)

特開2001-51903

【図4】



【図9】



【図7】

ディレクトリ デスクリプション

共通仕様

Byte(e)	Description	Length
1-4	尚未未使用Memory量	4
5-20	Directory ID + Tag	16
21	Directory Type	1
22-27	Time Stamp(yyyy, MM, dd, hh, mm)Option	6
28-29	RFU	2
30	次に續くApplication用のFile Data長	1

A

各Application用の仕様

Byte(e)	Description	Length
31	Directory Characteristics	1
32-33	Sub-Directory数	2
34-35	現状Directory下のFile数	2
36	PIN, Unblocking PIN, Administrative Code, 数	1
37	RFU	1
38	PIN 1 Status	1
39	Unblocking PIN 1 Status	1
40	PIN 2 Status	1
41	Unblocking PIN 2 Status	1
42-48	Administrative Management Use	7

B

Directory/ Type Coding(例)
 00:RFU
 01:Directory
 02:Sub-Directory
 04:Data File

Directory Characteristics(例)
 Bit 1:Clock Stop Mode
 Bit 2:RFU
 Bit 3-4:Clock Stop Mode
 Bit 5-7:RFU
 Bit 8:PIN 1 有効/無効

Security Status(例)
 Bit 1-4:PIN入力Counter
 0はBlockされている事を示す。
 Bit 5-7:RFU
 Bit 8:初期化情報

E

(18)

特開2001-51903

【図8】

ファイル デクリプション

共通仕様

Byte(s)	Description	Length
1-4	File Size	4
5-20	File ID + Tag	16
21	File Type	1
22-27	Time Stamp(yyyy, MM, dd, hh, mm)Option	6
28	Mode	1
29-32	Access Conditions	4
33	File Status	1
34	次に続くApplication用のFile Data長	1

各Application用の仕様

Byte(s)	Description	Length
35	Structure of Data File	1
36-37	Length of Record	2

File Type Coding(例)

C 00:RFU
01:Directory
02:Sub-Directory
04:Data File

D Mode(例)
00:RFU
01:INCREASE Command
Enable/Disable for Cyclic File

Mode(例)

E Bit 1-7:RFU
Bit 8:INCREMENT Command
Allowed or Not

Access Condition Code(例)

F 0:ALWAYS
1:PIN 1
2:PIN 2
3:RFU
4:ADM(Interactive)
5:ADM
6:NEVER

Byte 29(例)

G Bit 1-4:UPDATE
Bit 5-8:READ:SEEK

Byte 30(例)

Bit 1-4:RFU
Bit 5-8:INCREASE

Byte 31(例)

Bit 1-4:INVALIDATE
Bit 5-8:REHABILITATE

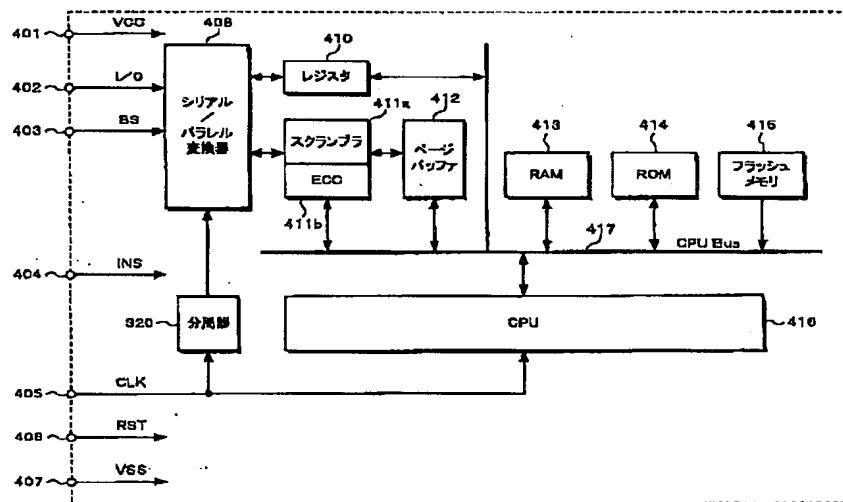
Byte 32(例)

Bit 1-4:SCRAMBLE
Bit 5-8:COPY

File Status(例)

G 00:Transparent
01:Linear Fixed
03:Cyclic

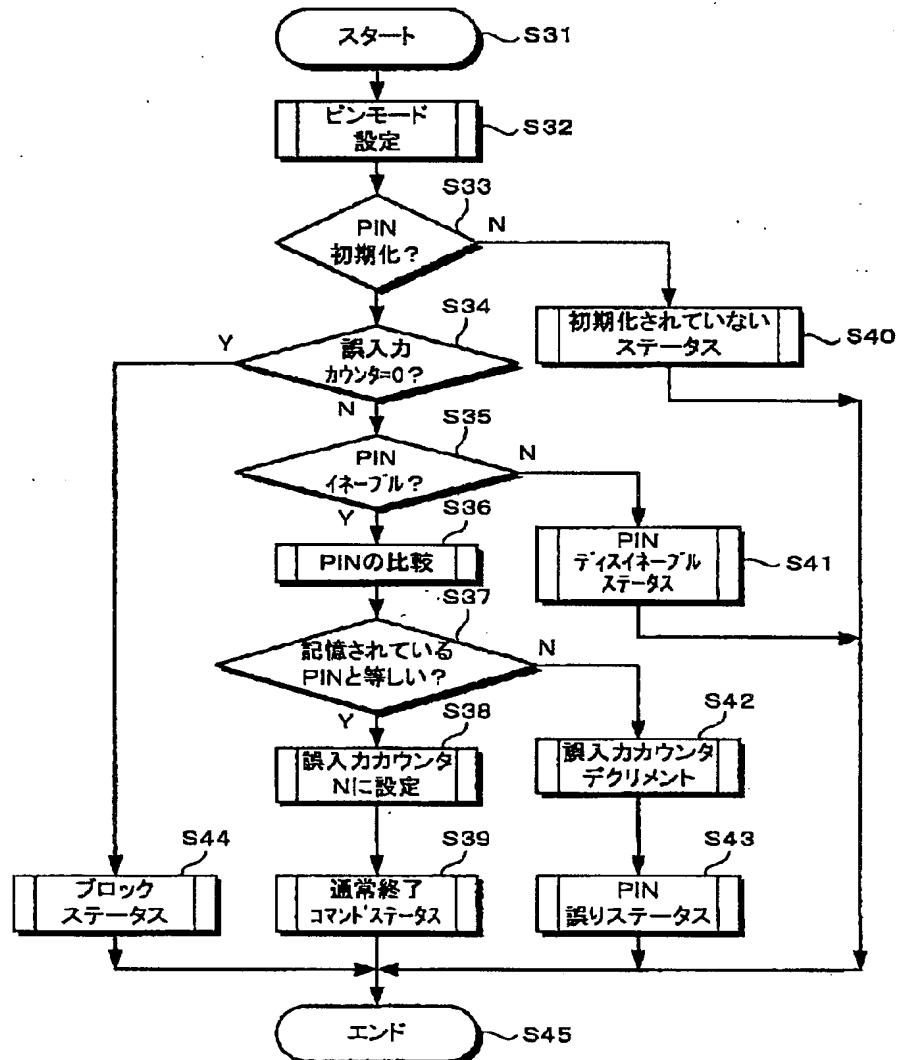
【図12】



(19)

特開2001-51903

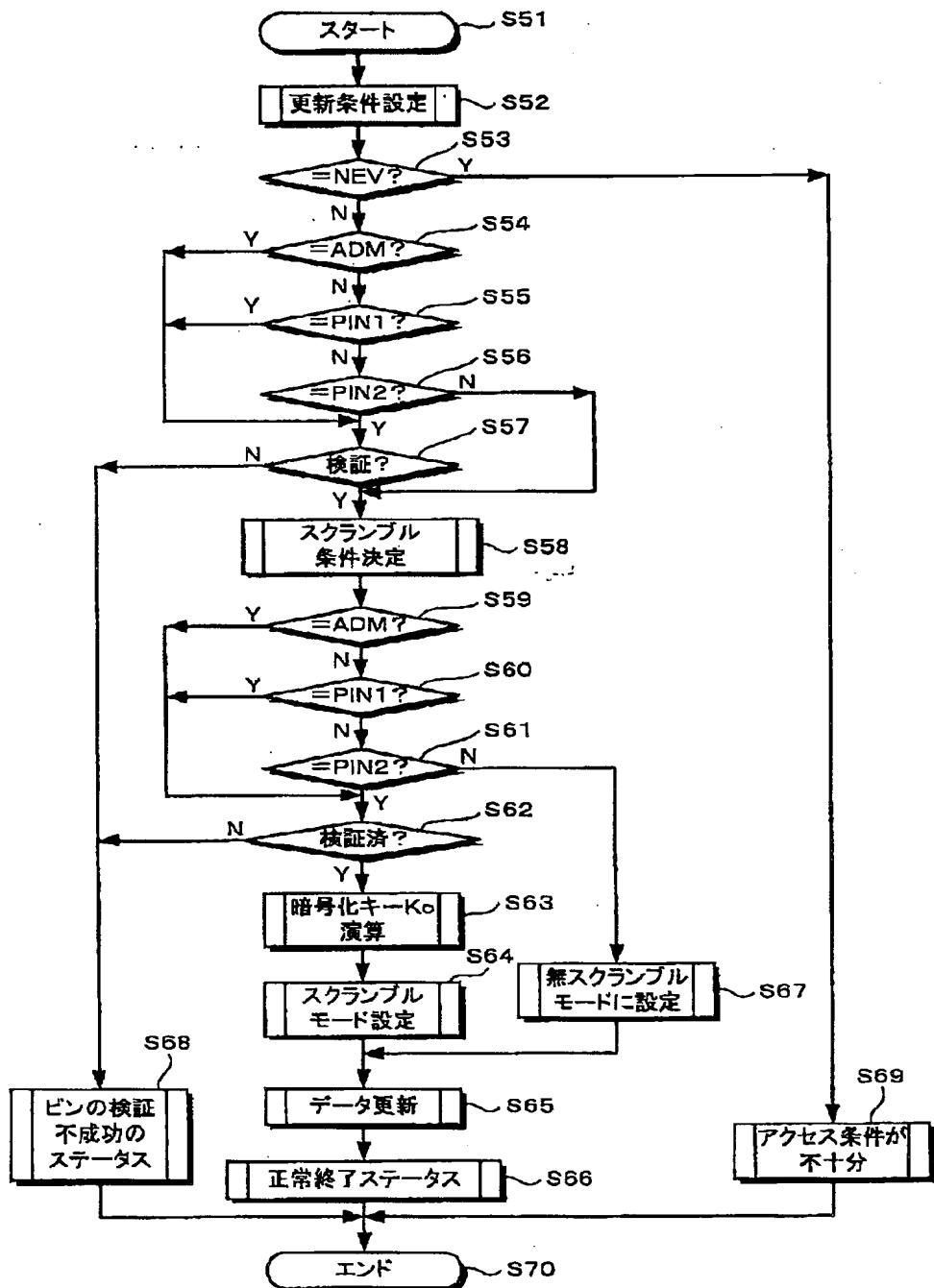
【図10】



(20)

特開2001-51903

【図11】



(21)

特開2001-51903

フロントページの続き

(51) Int. Cl. ¹	識別記号	F I	マークド(参考)
G 06 F 12/00	5 3 7	G 06 F 12/00	5 3 7 M
			5 3 7 A
			5 3 7 D
G 06 K 17/00		G 06 K 17/00	E
19/073		19/00	P

Fターム(参考) 5B017 AA01 AA06 BA05 BA07 BB03
BB08 CA07 CA08 CA11 CA12
CA14 CA15 CA16
5B035 AA13 AA14 BB09 BC00 CA39
5B058 CA23 KA33 KA35 YA16
5B082 AA11 CA07 EA01 GA02 GA14
GC05 JA08